Cuantumul primei amenzi pentru încalcarea GDPR ne plaseaza pe locul al doilea în Europa Centrala și de Est

Cel mai important moment pentru companiile din România dupa intrarea în vigoare a GDPR a fost cu siguranța data de 27 iunie 2019, când Autoritatea Națională de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP) a impus prima amenda, în cuantum de aproximativ 130.000 de euro, pentru încalcarea regulamentului 2016/679 de catre o instituție bancara.

Pentru ce a fost impusa amenda

La efectuarea unei plați, indiferent daca aceasta era inițiata de un titular de cont la banca sancționata sau de catre un terț utilizator al sistemului de plați interbancar, CNP-ul și adresa platitorului erau accesibile beneficiarului plații prin extrasul de cont sau prin detaliile plații oferite de banca. În urma investigației, ANSPDCP a concluzionat ca prelucrarea acestor date încalca principiul *data privacy by design*, conform caruia operatorii au obligația ca, de la momentul creionarii procesului de prelucrare și pâna la finalizarea acestuia, sa implementeze masuri tehnice și organizatorice adecvate în raport cu natura și riscurile prelucrarii, precum și cu posibilitațile tehnologice și financiare, pentru a asigura respectarea GDPR.

Principiul *data privacy by design* – implicații juridice și asupra sistemelor IT

Principiul *data privacy by design* activeaza ca o umbrela și presupune încorporarea celorlalte principii din GDPR sub o singura prevedere – spre exemplu, principiul minimizarii datelor. Conformarea cu data privacy by design implica o etapa preliminara de evaluare a riscului prelucrarii, prin intermediul careia operatorii identifica eventuale masuri de implementat. Mai mult decât atât, pe lânga evaluarea de natura juridica (de exemplu, identificarea datelor prelucrate ca fiind necesare în raport cu scopurile, perioada de retenție, temeiul utilizat etc.), acest principiu presupune verificarea temeinica a infrastructurii IT (sisteme, aplicații etc.), urmata de remodelarea acesteia, în cazul în care se identifica neconformitați. Astfel, respectarea *data privacy by design* nu se va putea realiza prin simpla adoptare a unor proceduri și politici, ci numai prin implementarea și testarea periodica a bunei funcționari a modificarilor sistemice ce asigura respectarea procedurilor și politicilor în materie de protecție a datelor.
Implementarea unui nou proces de business sau a unui nou software în cadrul companiei ar trebui facuta cu sprijinul responsabililor de protecția datelor.
Cea mai buna metoda de a verifica daca atât controalele tehnice, cât și cele non-tehnice funcționeaza este de a simula periodic un incident cibernetic ce are ca rezultat accesul neautorizat la date cu caracter personal.

Pentru a efectua acest exercițiu, echipa trebuie sa identifice datele care au fost accesate, sistemele ce stocau aceste informații și procesele de business afectate. Acest tip de test va obliga echipele interne sa verifice daca informațiile existente sunt de actualitate.

În mod similar, în urma acestor exerciţii, companiile pot identifica procese sau aplicaţii ce permit unor furnizori externi accesul la date, acces care poate nu a fost documentat în prealabil sau care nu este justificat. Totodata, pentru procesele ce au fost documentate corespunzator la momentul implementarii, o companie poate realiza ca informaţiile existente necesita un nivel mai ridicat de detalii.

În ceea ce priveşte proporţionalitatea amenzii, este interesant de menţionat faptul ca încalcarea principiului *data privacy by design* este încadrata de GDPR la o amenda de maximum 10 milioane de euro sau 2% din cifra de afaceri globala anuala, şi nu la pragul superior de 20 de milioane de euro sau 4%. În plus, în individualizarea cuantumului amenzii, ANSDPCP a trebuit sa aiba în vedere numarul mare de persoane vizate – 337.042 - şi alte aspecte, precum categoriile de date implicate, intenţia sau caracterul neglijent al faptei operatorului, potenţiale acţiuni de diminuare a prejudiciului suferit de persoanele vizate etc.

România, a doua cea mai mare amenda din Europa Centrala şi de Est

Raportata la amenzile acordate în Europa Centrala şi de Est, sancţiunea impusa de ANSPDCP este a doua cea mai mare dupa amenda emisa, dupa cea de 220.000 de euro din Polonia cu privire la cazul Bisnode, care utiliza date cu caracter personal din surse publice fara respectarea obligaţiilor de informare a persoanelor vizate. Astfel, în baza unui studiu efectuat de Deloitte Legal în Europa Centrala şi de Est, cuantumul acestei prime amenzi situeaza România în topul amenzilor acordate în acest prim an de aplicare a GDPR. Studiul mai releva ca, în Bulgaria, cea mai mare amenda nu a depaşit 27.000 de euro, în Ungaria, 40.000 de euro, iar în Lituania, 61.500 euro.

Industria financiar-bancara a fost printre cele mai vizate de investigaţiile ANSPDCP, atât înainte, cât şi dupa intrarea în vigoare a GDPR. Mai mult decât atât, ANSPDCP a comunicat ca plângerile şi sesizarile primite au avut în vedere încalcarea principiilor de prelucrare a datelor personale în sistemul bancar şi a regulilor de confidenţialitate şi securitate a prelucrarilor de date personale.

Consecinţe în plan procedural şi judiciar

Din datele oficiale comunicate de ANSPDCP, la finalul lunii mai 2019 se aflau în desfaşurare aproximativ 1.000 de investigaţii şi este de aşteptat ca entitaţile ce vor fi supuse unor sancţiuni şi masuri corective sa conteste în instanţa aceste decizii.

Contestaţiile înregistrate pe rolul secţiilor de contencios administrativ şi fiscal ale tribunalelor suspenda doar plata amenzii, nu şi obligaţia de a aplica masuri corective, aşadar cel mai probabil acestea vor fi dublate de cereri de suspendare a masurilor corective, în temeiul prevederilor din Legea contenciosului administrativ.
În lipsa unei jurisprudenţe cristalizate pe diferitele tipologii de încalcari aduse legislaţiei în materie, generata şi de faptul ca legislaţia anterioara prevedea praguri semnificativ mai mici pentru amenzi (aprox. 10.000 de euro), va trebui ca instanţele de judecata sa stabileasca o optica proprie în soluţionare acestor cauze. Vom avea, deci, o potenţiala practica neunitara la nivel naţional.

La scurt timp de la prima amenda, ANSPDCP a anunţat înca doua sancţiuni, în valoare de 15.000 şi respectiv de 3.000 de euro. Ramâne de vazut daca valoarea şi frecvenţa acestora va creşte, având în vedere apetitul persoanelor vatamate de a formula şi acţiuni directe în instanţa (acţiuni scutite de plata taxei de timbru), cât timp introducerea unor astfel de acţiuni nu împiedica sesizarea, în paralel, a ANSPDCP şi nici nu obliga ANSPDCP la suspendarea sau clasarea plângerilor.